Abstract of the Disclosure

Secure computation environments are protected from bogus or rogue load modules, executables and other data elements through use of digital signatures, seals and certificates issued by a verifying authority. A verifying authority - which may be a trusted independent third party — tests the load modules or other executables to verify that their corresponding specifications are accurate and complete, and then digitally signs the load module or other executable based on tamper resistance work factor classification. Secure computation environments with different tamper resistance work factors use different verification digital signature authentication techniques (e.g., different signature algorithms and/or signature verification keys) — allowing one tamper resistance work factor environment to protect itself against load modules from another, different tamper resistance work factor environment. Several dissimilar digital signature algorithms may be used to reduce vulnerability from algorithm

compromise, and subsets of multiple digital signatures may be used to reduce the scope of any specific compromise.